PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : H04K 1/00

A1

(11) International Publication Number: WO 89/ 07375

(43) International Publication Date: 10 August 1989 (10.08.89)

(21) International Application Number: PCT/US89/00002

(22) International Filing Date: 3 January 1989 (03.01.89)

(31) Priority Application Number: 150,876

(32) Priority Date: 1 February 1988 (01.02.88)

(33) Priority Country: US

(71) Applicant: MOTOROLA, INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

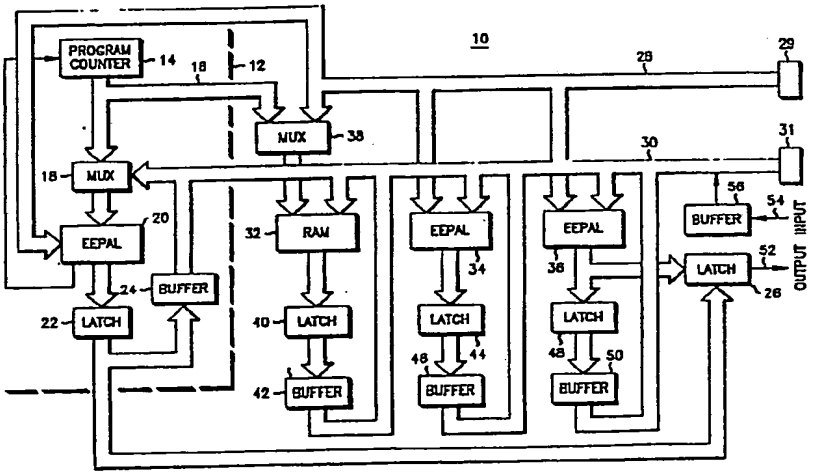
(72) Inventors: DABBISH, Ezzat, A. ; 700 Thompson Blvd., Buffalo Grove, IL 60089 (US). BYRNS, John, P. ; 1953 Governors Lane, Hoffman Estates, IL 60195 (US). MCCLAUGHRY, Michael, J. ; 114 Perth Road, Cary, IL 60013 (US). PUHL, Larry, C. ; 6 Plum Court, Sleepy Hollow, IL 60118 (US). BROWN, Daniel, P. ; 788 Chatham Avenue, Elmhurst, IL 60126 (US). ZIOLKO, Eric, F. ; 810 S. Pheasant Walk Drive, Schaumburg, IL 60193 (US). BRIGHT, Michael, W. ; 1339 N. Mitchell Avenue, Arlington Heights, IL 60004 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola, Inc., Intellectual Property Department, 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), DK, FR (European patent), GB (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: CRYPTOGRAPHIC METHOD AND APPARATUS WITH ELECTRONICALLY REDEFINABLE ALGORITHM



(57) Abstract

A cryptographic apparatus (10) for encrypting and decrypting digital words includes a mechanism that permits a cipher algorithm to be electronically stored after the manufacture of the apparatus. The storing mechanism includes at least one electrically erasable, programmable gate array (34, 36) containing a portion of the cipher algorithm and at least one random access memory device (32) coupled to the array for storing digital data generated by the algorithm. A mechanism (12) which is coupled to the gate array and memory device controls the execution of the algorithm for each digital word thereby decrypting encrypted digital words and encrypting non-encrypted digital words.

BEST AVAILABLE COPY

This Page Blank (uspto)

⑲日本国特許庁(JP)　　⑪特許出願公表

⑫公表特許公報(A)　　平3−500117

⑬公表　平成3年(1991)1月10日

⑤Int. Cl.⁵	識別記号	庁内整理番号	審査請求 有
H 04 L 9/06 9/14			予備審査請求 有　部門(区分) 7(3)
		6914−5K　H 04 L 9/02	Z

(全 8 頁)

⑭発明の名称　電子的に再定義可能なアルゴリズムを備えた暗号化方法および装置

⑳特　願　平1−501798
㉒㉒出　願　昭64(1989)1月3日
㉕翻訳文提出日　平2(1990)7月30日
㉖国際出願　PCT/US89/00002
㉗国際公開番号　WO89/07375
㉘国際公開日　平1(1989)8月10日

優先権主張　㉜1988年2月1日㉝米国(US)㉞150,876

⑦発明者　ダビッシュ・エザート　エイ　アメリカ合衆国イリノイ州　60089、バッファロー・グルーブ、トンプソン・プルバード　700
⑦発明者　バインズ・ジョン　ビー　アメリカ合衆国イリノイ州　60195、ホフマン・エステイツ、ガバナーズ・レーン　1953
⑦出願人　モトローラ・インコーポレーテッド　アメリカ合衆国イリノイ州　60196、シャンバーグ、イースト・アルゴンクイン・ロード　1303
⑦代理人　弁理士　池内　義明

⑧指定国　AT(広域特許),BE(広域特許),CH(広域特許),DE(広域特許),DK,FR(広域特許),GB(広域特許),IT(広域特許),JP,KR,LU(広域特許),NL(広域特許),SE(広域特許)

最終頁に続く

請求の範囲

1．デジタルワードを暗号化しかつ解読するための暗号装置であって、該装置は、

暗号アルゴリズムを電子的に格納するための手段であって、該格納手段は前記アルゴリズムの一部を含む少なくとも1つの電気的にプログラム可能なアレイ論理装置および該論理装置に結合され前記アルゴリズムによって発生されるデジタルデータを格納するための少なくとも1つのランダムアクセスメモリ装置を有するもの、そして

前記論理装置およびメモリ装置に結合され前記デジタルワードの各々に対する前記アルゴリズムの実行を制御し、それにより暗号化されたデジタルワードを解読しかつ暗号化されていないデジタルワードを暗号化するもの、

を具備する暗号装置。

2．前記論理装置は消去可能である請求の範囲第1項に記載の暗号装置。

3．前記論理装置は電気的に消去可能である請求の範囲第2項に記載の暗号装置。

4．前記制御手段は他の電気的にプログラム可能なアレイ論理装置を具備する請求の範囲第1項に記載の暗号装置。

5．さらに、前記アレイ論理装置、メモリ装置および前記制御手段に結合された共通のデジタルアドレスおよびデータバスを具備し、該アドレスおよびデータバスは各々前記アレイ論理装置、メモリ装置、および制御手段が外部プログラム装置によってプログラムされて暗号アルゴリズムを実行することを許容する通信ポートを有する請求の範囲第1項に記載の暗号装置。

6．さらに、前記1つのアレイ論理装置、他のアレイ論理装置、メモリ装置および前記制御手段に結合された共通のデジタルアドレスおよびデータバスを具備し、前記アドレスおよびデータバスは各々前記1つの論理装置、他の論理装置、メモリ装置、および制御手段が外部プログラム装置によってプログラムされて暗号アルゴリズムを実行することを許容する通信ポートを有する請求の範囲第4項に記載の暗号装置。

7．前記制御手段はマイクロプロセッサを含まない請求の範囲第1項に記載の暗号装置。

8．受信された暗号化信号を復調して入り暗号化デジタルワードを提供するための手段、

出暗号化デジタルワードに対応する変調された信号を発生するための手段、

前記入り暗号化デジタルワードを解読しかつ前記出暗号化デジタルワードを非暗号化デジタルワードから発生するための暗号手段、

を具備し、前記暗号手段は、

暗号アルゴリズムを電子的に格納するための手段であっ

て、該格納手段は前記アルゴリズムの一部を含む少なくとも１つの電気的にプログラム可能なアレイ論理装置および前記論理装置に結合され前記アルゴリズムによって発生されるデジタルデータを格納するための少なくとも１つのランダムアクセスメモリ装置を有するもの、そして

前記論理装置およびメモリ装置に結合され前記入り暗号化デジタルワードを解読しかつ非暗号化デジタルワードに基づき前記出暗号化デジタルワードを発生するための前記アルゴリズムの実行を制御するための手段、

を具備する２方向通信装置。

９．前記論理装置は消去可能である請求の範囲第８項に記載の通信装置。

１０．前記論理装置は電気的に消去可能である請求の範囲第９項に記載の通信装置。

１１．前記制御手段は他の電気的にプログラム可能なアレイ論理装置を具備する請求の範囲第８項に記載の通信装置。

１２．さらに、前記アレイ論理装置、メモリ装置および前記制御手段に結合された共通のデジタルアドレスおよびデータバスを具備し、該アドレスおよびデータバスは各々前記アレイ論理装置、メモリ装置、および制御手段が外部プログラム装置によってプログラムされて暗号アルゴリズムを実行することを許容する通信ポートを有する請求の範囲第８項に記載の通信装置。

１３．さらに、前記１つのアレイ論理装置、他のアレイ論理装置、メモリ装置および前記制御手段に結合された共通のデジタルアドレスおよびデータバスを具備し、前記アドレスおよびデータバスは各々前記１つのアレイ論理装置、他のアレイ論理装置、メモリ装置、および制御手段が外部プログラム装置によってプログラムされて暗号アルゴリズムを実行することを許容する通信ポートを有する請求の範囲第１１項に記載の通信装置。

１４．前記制御手段はマイクロプロセッサを含まない請求の範囲第８項に記載の通信装置。

１５．前記装置は前記暗号化信号を受信する受信機および前記変調された信号を送信する送信機を含む２方向ワイヤレス無線送受信機を具備する請求の範囲第８項に記載の通信装置。

１６．暗号装置を含む通信装置を製造するための方法であって、

前記暗号装置を前記通信装置に導入する段階であって、前記暗号装置は導入の時には使用されるべき暗号アルゴリズムを含まないもの、

前記暗号装置に該装置が試験されることを許容する試験アルゴリズムをロードする段階、

前記通信装置および暗号装置を適正な動作のために試験する段階、そして

前記導入および試験に続き、前記試験アルゴリズムを消去しかつ前記暗号装置内の論理ゲートの相互接続を電子的に再規定し使用されるべき暗号アルゴリズムの部分を形成するプール代数機能を達成する段階、

を具備し、それにより前記通信装置および暗号装置が前記プール代数機能の規定に先立ち暗号アルゴリズムの安全性を実質的に容することのない通信装置の製造方法。

１７．前記消去段階は電子的に前記試験アルゴリズムを消去する段階を備えた請求の範囲第１６項に記載の方法。

１８．さらに、消去可能な、プログラム可能アレイ論理装置を電子的にプログラムして前記プール代数機能を含ませる段階を備えた請求の範囲第１６項に記載の方法。

１９．さらに、前記暗号アルゴリズムを前記暗号装置内に含まれる共通のデジタルアドレスおよびデータバスにより前記暗号装置にロードする段階を具備し、前記プール代数機能は前記暗号装置内の前記バスに結合された消去可能、プログラム可能アレイ論理装置に電子的に規定される請求の範囲第１６項に記載の方法。

明　細　書

電子的に再定義可能なアルゴリズムを備えた暗号化方法および装置

発明の背景

この発明は一般的にはデジタル暗号装置の分野に向けられており、かつより特定的にはそれにより暗号アルゴリズムが暗号装置に格納されるアーキテクチャおよび方法に向けられている。この発明はまた暗号化通信機器の製造後に暗号アルゴリズムを暗号化装置にロードする結果として保安されていない環境で暗号化通信機器を製造することができる方法に向けられている。

典型的な暗号化装置においては、秘密のキーがメッセージを暗号化しかつ解読するために暗号アルゴリズムと組合わせて利用されている。該キーは安全性を増強するために望むだけ頻繁に変えることができる。

特定のキーを用いてメッセージが暗号化されかつ暗号解読されるステップからなる暗号アルゴリズムは高いレベルの安全性（security）を維持するためにしばしば保護される。もし該アルゴリズムが知られると、メッセージとキーのみがその時知られていないことになるから符号化されたメッセージを解読することはより容易になる。従って、最大の安全性を要する応用に対しては、アルゴリズムそれ自

体が保護されることが重要である。

アルゴリズムが存在する電子回路は通信されるメッセージを傷つけるようなものでないよう設計されることも重要である。論理ハードウェアに格納されているアルゴリズムはソフトウェアで格納されているアルゴリズムより「フェイルセーフ」にすることはより容易である。暗号アルゴリズムを含む論理ハードウェアおよびそれを含む機器の製造はしばしば厳格にコントロールされる。そのような固定された暗号化論理を含む通信機器の製造は暗号化を用いない通信機器と比較してかなりの付加的な手順を要求する。これは厳格なコントロールおよび実質的に増大された製造コストが必要な結果となる。

発明の目的

本発明の目的は、暗号アルゴリズムが電子的に装置の製造の後にかつ暗号化装置を利用する通信機器の製造の後に入力されることを許容するアーキテクチャを有する暗号化装置を提供することにある。

この発明の他の目的は、そのような機器の製造の間に保安のコントロール手法を用いる必要がない暗号化通信機器の製造のための改良された方法を提供することにある。

図面の簡単な説明

第１図は、本発明に係わる暗号化装置の１実施例を示すブロック図である。

第２図は、本発明に係わる暗号化装置を導入した通信機器を示すブロック図である。

詳細な説明

第１図は、本発明に従いその製造の後に暗号アルゴリズムが電子的に規定できる暗号装置の実施例１０を示す。点線で左図に示されたシーケンスコントローラ１２は出力がバス１６によってマルチプレクサ１８に結合されたプログラムカウンタ１４を含む。マルチプレクサ１８の出力は電子的消去可能、プログラム可能アレイ論理装置（ＥＥＰＡＬ）２０に結合されている。そのようなＥＥＰＡＬ装置は商業的に入手可能でありかつ電子的にプログラムして互いに相互接続し入力データに対して動作するブール代数式により決定される出力を生成することができる数多くの論理ゲートからなる。ここで用いられているように、アレイ論理装置はマイクロプロセッサを含まない。アレイ論理装置は電子的にプログラム可能でありかつ好ましくは再プログラムを許容するため消去可能であることが重要である。装置２０の出力はラッチ２２によってバッファ２４へかつラッチ２６へ結合されている。装置２０の出力はまたプログラムカウンタ１４へのクロック入力を提供しこれは該カウンタを周期的に増分しかつ予めプログラムされた数のステップを通り移行（ステップ）させる。

シーケンスコントローラ１２の一般的な目的は第１図に示された回路の残りのサイクリックな動作シーケンスを制御すること、即ち暗号アルゴリズムをステップバイステップのベースで実施することである。通信ポート２９を備えた共通アドレスバス２８および通信ポート３１を備えたデータバス３０はＥＥＰＡＬ２０、ランダムアクセスメモリ（ＲＡＭ）装置３２、そしてＥＥＰＡＬ３４および３６に対しデジタル通信経路を確立する。ＲＡＭ３２はマルチプレクサ３８によってアドレスされ、該マルチプレクサ３８はプログラムカウンタ１４の出力１６またはアドレスバス２８の間で選択する。データはデータバス３０によってＲＡＭ３２に入力される。特定アドレスに格納されたデータ情報はＲＡＭ３２からラッチ４０およびバッファ４２によってデータバス３０に結合される。

ＥＥＰＡＬ３４はそれぞれのバスからのアドレスおよびデータ入力を有している。ＥＥＰＡＬ３４からの出力はラッチ４４およびバッファ４６によってデータバス３０に結合されている。同様にして、ＥＥＰＡＬ３６はアドレスおよびデータ入力をそれぞれのバスラインから受け取る。その特定のゲート構成によって決定されるその出力はラッチ４８およびバッファ５０によってデータバス３０に結合される。その出力はまたラッチ２６に結合されかつラッチ２２の出力を介してラッチ２６に通信されるプログラムシーケンスの終わりで暗号化デジタル出力５２を規定する。

暗号化されるべきデジタル情報は入力５４によりバッファ５６に結合され該バッファ５６は次に該情報をデータバス３０に結合する。該デジタル情報は１つまたはそれ以上のビットを有するデジタルワードからなる。暗号化装置１０による入力データの暗号化は実時間のメッセージフローを維持するために暗号化されるべき次の情報の入力の前に達成されなければならないことが理解される。従って、第１図に示される要素にクロック情報を提供するクロック（図示せず）は入力時間フレーム内に暗号アルゴリズムにより必要とされる数のステップが完了されることを許容するために充分なレートのものでなくてはならない。

本発明の重要な見地の１つは暗号アルゴリズムが該アルゴリズムを実行するハードウェアの製造の後に規定できる能力である。第１図に示された好ましい実施例はこの目標を電子的に消去可能な、プログラム可能アレイ論理装置およびランダムアクセスメモリの使用により達成する。暗号化装置１０の製造およびその通信機器への挿入の後に、マイクロプロセッサにより制御されるコンピュータのような外部装置がアドレスおよびデータバスポートに結合されかつ各ＥＥＰＡＬの内部ゲート構成を試験アルゴリズムによってプログラムしかつＲＡＭ３２に格納される初期試験データを規定するために利用される。試験が完了した後、通信機器は試験プログラムを依然として暗号化装置内に有したまま顧客に届けられ、それにより完成したユニットが保

安手段を使用することなく取り扱いできるようになる。顧客は次に暗号化装置に同様の外部コンピュータを用いることにより暗号アルゴリズムをロードする。

暗号アルゴリズムは試験アルゴリズムに基づき決定できないから、実際の暗号アルゴリズムが外部的にプログラムされる時にそのような機器の厳格な保安コントロールをする必要はない。このことは暗号化ハードウェアと共に該ハードウェアを含む機器を厳格な保安コントロール環境なく製造することを許容する。

暗号装置１０の動作をより良く理解するため、次に例示的な説明を行なう。ＥＥＰＡＬを規定しかつ初期データをＲＡＭにロードするためにプログラムされている外部コンピュータがアドレスおよびデータバスに結合される。ＥＥＰＡＬは各々特定のブール代数機能を達成するため順次的にプログラムされる。キーおよび初期データはＲＡＭ３２に格納される。該装置は今や、それが所望の暗号アルゴリズムを含んでいるから、入力５４における入りデータを処理する用意ができている。

最初の入力データバイトまたはワードはＲＡＭ３２に格納される。ＲＡＭ３２に格納されたキーおよび入力データは入力データとしてＥＥＰＡＬ３４に転送され、該ＥＥＰＡＬ３４はそのようなデータに作用して結果として得られる出力データＲ１を生成する。この結果として得られたデータＲ１はＲＡＭ３２に格納される。初期データおよび前記結果として得られたデータＲ１はＲＡＭ３２からＥＥＰＡＬ３６に転送され、ＥＥＰＡＬ３６はこれらの入力に対して出力データＦを生成するよう作用する。この出力データＦはＲＡＭ３２に格納されかつ初期データの代りに置換えられ、それによりそれが暗号化されるべき次の入力データに対するものに代って使用される。同時に、データＦがラッチ２６に転送されかつライン５２において暗号化出力データとしてクロック出力される。反復的な処理が各々の新しい入力データバイトに対して行なわれ対応する出力暗号化データを生成する。

上記の例は可能な暗号化の応用を示す。ＲＡＭ３２が利用できるから、中間的生成物が格納できかつ使用される数学的関数の複雑性に応じて種々の方法でその後の計算のために後に使用できることが明らかであろう。必要とされる保安のレベル、要求される繰り返しの数、そして処理された暗号化が生じなければならない速度に応じて、より多くあるいはより少ないＥＥＰＡＬを用いることができる。

本発明の他の利点はシフトレジスタのような交番的格納装置の代りにＲＡＭ３２を使用することにある。ＲＡＭはプログラム可能なレジスタとして機能することができ、それにより何らかのプロセスの間に格納することができるバイト数をＲＡＭの制限容量内で変えることが許容される。これはそのような装置に保安の程度を追加するがそれは使用されている計算のバイト数また長さを決定することの困難性を増大するからである。

本発明に係わる暗号化装置はまた同様の暗号化技術を達成するために汎用のマイクロプロセッサまたはより特別のデジタル信号プロセッサの使用と対照することができる。そのような代替物を用いることはできるが、マイクロプロセッサの比較的複雑な内部構造はそのような代替物を「フェイルセーフ」のために設計することを困難にする。即ち、利用されるアルゴリズムを妥協することなくメッセージの安全性を保護する許容できる様式でないということである。本発明に係わるより直接的な機能装置が故障の際により容易に保護されかつ診断できる。

第２図は、本発明に係わる暗号化装置１０を導入した２方向無線機からなる通信機器を示す。アンテナ６０が音声情報を搬送する信号を送受切換器およびフィルタ６２に結合し、該フィルタ６２は受信信号をミキサ６４に結合する。発振器６６からミキサ６４への他の信号が混合されて結果的に中間周波出力６８が生成される。６８および復調器７０の間の伝統的な受信機回路は図示されていない。該復調器は出力をマルチプレクサ７２に提供し、該マルチプレクサ７２は受信された暗号化信号をデジタル入力５４として暗号化装置１０に導く。該装置１０からの暗号解読された出力５２はマルチプレクサ７４によりデジタル－アナログコンバータ７６に結合される。コンバータ７６からのアナログ出力はオーディオ増幅器７８により増幅されその後スピーカ８０に結合される。

受信された信号は対応する暗号アルゴリズムおよびキーを利用する遠隔の無線機における対応する暗号化装置１０によって暗号化されているであろう。この例においては、回復されたデータは装置１０により暗号解読されかつアナログ信号に変換されて聴取者に明瞭なテキスト音声メッセージを提供する。

暗号化されたメッセージを送信するためには、音声信号がマイクロホン８２によってオーディオ増幅器８４に結合され、該オーディオ増幅器８４の出力はアナログ－デジタルコンバータ８６によりデジタル信号に変換される。このコンバータの出力はマルチプレクサ７２により暗号化装置１０に結合され、該暗号化装置１０は入力データを暗号化しかつマルチプレクサ７４によって送信機の変調器８８に結合される出力５２を提供する。変調器８８および電力増幅器９０の間に通常見られる伝統的な送信機段は図示されていない。増幅器９０からの増幅された信号はフィルタ６２を通りアンテナ６０に結合され、そこで該信号は同様の暗号化装置１０を有する対応する受信機に送信される。

先に説明したように、そのような無線機の製造はもし暗号化装置１０が無線機の製造中に暗号アルゴリズムを含んでおれば保安および処理報告(accounting)手順を必要とするであろう。本発明は暗号アルゴリズムを後の時間にロードすることを許容するから、暗号化装置１０を含む無線機

は既特に保安された状況にない工場環境で設定することができる。

第２図において無線送受信機が暗号化装置を導入したものとして示されたが、モデムおよび保安電話のような、音声またはデータを伝達するよう設計される他の通信機器も同様に本発明に係わる暗号化装置を用いることができることは明らかであろう。

本発明の１実施例がここに示されかつ説明されたが、本発明の範囲は以下の請求の範囲によって規定される。

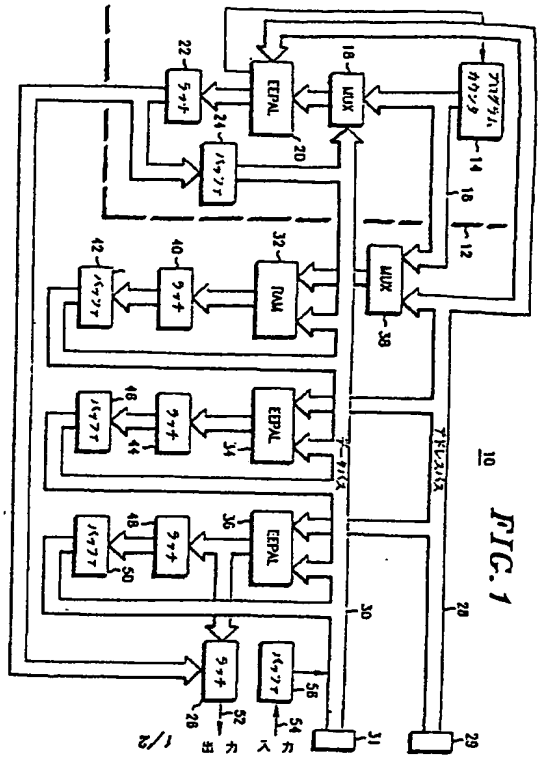


FIG. 1

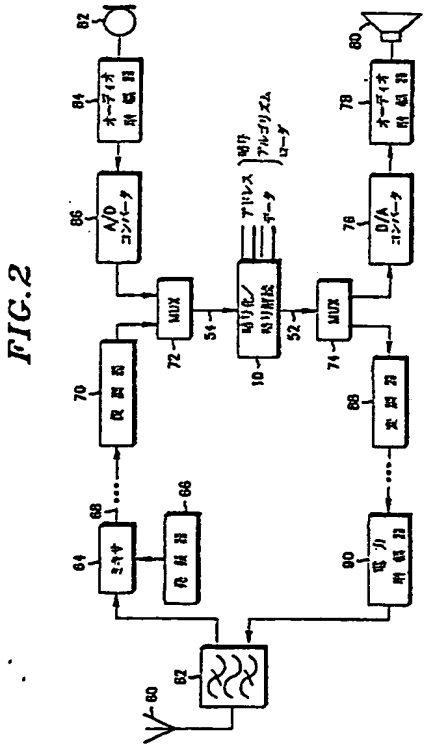


FIG. 2

補正書の写し（翻訳文）提出書（特許法第１８４条の８）

平成２年７月３０日

特許庁長官　植　松　敏　殿

１．特許出願の表示
PCT／US89／00002

２．発明の名称
電子的に再定義可能なアルゴリズムを備えた暗号化方法および装置

３．特許出願人
住　所　アメリカ合衆国イリノイ州 60196、シャンバーグ、イースト・アルゴンクイン・ロード 1303
名　称　モトローラ・インコーポレーテッド
代表者　ラウナー・ビンセント　ジェイ

４．代　理　人
住　所　〒231 神奈川県横浜市中区本町１丁目７番地 東ビル　電話 045(211)2795 池内国際特許事務所
氏　名　（８３５７）弁理士　池　内　寛　明

５．補正書の提出年月日　１９８９年１２月１２日

６．添付書類の目録
補正の内容説明書　１通
補正書の写し（翻訳文）　１通

方式審査

特許庁 27.3 国際出願

補正請求の範囲

1．（削除）
2．（削除）
3．（削除）
4．（削除）
5．（削除）
6．（削除）
7．（削除）
8．（補正）受信された暗号化信号を復調して入り暗号化デジタル情報を提供するための手段、
出暗号化デジタル情報に対応する変調された信号を発生するための手段、
前記入り暗号化デジタル情報を解読しかつ前記出暗号化デジタル情報を非暗号化デジタル情報から発生するための暗号手段、
を具備し、前記暗号手段は、
デジタル情報、反復中間データ、および少なくとも1つのキーを格納するためのランダムアクセスメモリ手段、
該ランダムアクセスメモリ手段に作動的に結合され、前記デジタル情報、反復中間データ、および前記少なくとも1つのキーにブール代数機能を行ない出力データおよび反復中間データを出力する再プログラム可能論理手段、
前記再プログラム可能論理手段およびランダムアクセスメモリ手段に作動的に結合され、前記ランダムアクセスメモリ手段へのデジタル情報の入力を制御し、前記デジタル情報、反復中間データ、および前記少なくとも1つのキーのランダムアクセスメモリ手段から再プログラム可能論理手段への転送を制御し、前記反復中間データのプログラム可能論理手段からランダムアクセスメモリ手段への入力を制御し、前記再プログラム可能論理手段によるブール代数機能の達成を制御し、かつ前記再プログラム可能論理手段からの出力データの出力を制御するための再プログラム可能コントローラ手段、そして
前記再プログラム論理手段、前記ランダムアクセスメモリ手段、および前記再プログラム可能コントロール手段に作動的に結合され、前記デジタル情報が前記暗号装置に入力されかつ暗号化されたまたは暗号解読された情報が前記暗号装置から出力されるように入力および出力デジタル通信経路を提供し、かつ前記再プログラム可能論理手段および前記再プログラム可能コントロール手段が外部装置によってプログラム可能なように通信経路を提供するための通信手段、
を具備する2方向通信装置。
9．（削除）
10．（削除）
11．（削除）
12．（削除）
13．（削除）
14．（削除）
15．（削除）
16．（補正）暗号装置を含む通信装置を製造するための方法であって、
導入の時には前記暗号装置は使用されるべき暗号アルゴリズムを含まないように、前記暗号装置を前記通信装置に導入する段階、
前記暗号装置に該装置が試験されることを許容する試験アルゴリズムをロードする段階、
前記通信装置および暗号装置を適正な動作のために試験する段階、そして
前記導入および試験に続き、前記試験アルゴリズムを消去しかつ使用されるべき暗号アルゴリズムの少なくとも一部を形成するブール代数機能を達成するために前記暗号装置を再プログラムする段階、
を具備し、それにより使用されるべき暗号アルゴリズムが前記試験アルゴリズムに基づき決定できないようにした通信装置の製造方法。
17．前記消去段階は電子的に前記試験アルゴリズムを消去する段階を備えた請求の範囲第16項に記載の方法。
18．さらに、消去可能な、プログラム可能アレイ論理装置を電子的にプログラムして前記ブール代数機能を含ませる段階を備えた請求の範囲第16項に記載の方法。
19．さらに、前記暗号アルゴリズムを前記暗号装置内に含まれる共通のデジタルアドレスおよびデータバスにより前記暗号装置にロードする段階を具備し、前記ブール代数機能は前記暗号装置内の前記バスに結合された消去可能、プログラム可能アレイ論理装置に電子的に規定される請求の範囲第16項に記載の方法。
20．（追加）デジタル情報を暗号化しかつ解読するための暗号装置であって、
前記デジタル情報、反復中間データ、および少なくとも1つのキーを格納するためのランダムアクセスメモリ手段
該ランダムアクセスメモリ手段に作動的に結合され、前記デジタル情報、反復中間データ、および前記少なくとも1つのキーにブール代数機能を行ない出力データおよび反復中間データを出力する再プログラム可能論理手段、
前記再プログラム可能論理手段およびランダムアクセスメモリ手段に作動的に結合され、前記ランダムアクセスメモリ手段へのデジタル情報の入力を制御し、前記デジタル情報、反復中間データ、および前記少なくとも1つのキーのランダムアクセスメモリ手段から再プログラム可能論理手段への転送を制御し、前記反復中間データのプログラム可能論理手段からランダムアクセスメモリ手段への入力を制御し、前記再プログラム可能論理手段によるブール代数機能の達成を制御し、かつ前記再プログラム可能論理手段からの出力データの出力を制御するための再プログラム可

能コントローラ手段、そして

前記再プログラム論理手段、前記ランダムアクセスメモリ手段、および前記再プログラム可能コントロール手段に作動的に結合され、前記デジタル情報が前記暗号装置に入力されかつ暗号化されたまたは暗号解読された情報が前記暗号装置から出力されるように入力および出力デジタル通信経路を提供し、かつ前記再プログラム可能論理手段および前記再プログラム可能コントロール手段が外部装置によってプログラム可能なように通信経路を提供するための通信手段、

を具備する暗号装置。

２１．（追加）前記再プログラム可能論理手段は少なくとも１つの電子的にプログラム可能なアレイ論理装置を具備する請求の範囲第２０項に記載の暗号装置。

２２．（追加）前記通信手段は外部プログラム装置が前記再プログラム可能論理手段および再プログラム可能コントロール手段をプログラムすることを許容しかつ前記キーが入力されることを許容するアドレスバス、データバス、および通信ポートを具備する請求の範囲第２０項に記載の暗号装置。

２３．（追加）前記再プログラム可能論理手段は少なくとも１つの電子的に消去可能なプログラム可能アレイ論理（ＥＥＰＡＬ）装置を具備する請求の範囲第２０項に記載の暗号装置。

２４．（追加）少なくとも１つの前記ＥＥＰＡＬ装置は前記デジタル通信経路を介して外部プログラム装置によりプログラムされる請求の範囲第２３項に記載の暗号装置。

２５．（追加）前記再プログラム可能コントロール手段は少なくとも１つの電子的にプログラム可能なアレイ論理装置を具備する請求の範囲第２０項に記載の暗号装置。

２６．（追加）前記再プログラム可能コントロール手段は少なくとも１つの電子的に消去可能なプログラム可能アレイ論理（ＥＥＰＡＬ）装置を具備する請求の範囲第２０項に記載の暗号装置。

２７．（追加）少なくとも１つの前記ＥＥＰＡＬ装置は前記デジタル通信経路を介して外部プログラム装置によりプログラムされる請求の範囲第２６項に記載の暗号装置。

２８．（追加）前記再プログラム可能論理手段は少なくとも１つの電子的にプログラム可能なアレイ論理装置を具備する請求の範囲第８項に記載の２方向通信装置。

２９．（追加）前記通信手段は外部プログラム装置が前記再プログラム可能論理手段および再プログラム可能コントロール手段をプログラムすることを許容しかつ前記キーが入力されることを許容するアドレスバス、データバス、および通信ポートを具備する請求の範囲第８項に記載の２方向通信装置。

３０．（追加）前記再プログラム可能論理手段は少なくとも１つの電子的に消去可能なプログラム可能アレイ論理（ＥＥＰＡＬ）装置を具備する請求の範囲第８項に記載の２方向通信装置。

３１．（追加）少なくとも１つの前記ＥＥＰＡＬ装置は前記デジタル通信経路を介して外部プログラム装置によりプログラムされる請求の範囲第３０項に記載の２方向通信装置。

３２．（追加）前記再プログラム可能コントロール手段は少なくとも１つの電子的にプログラム可能なアレイ論理装置を具備する請求の範囲第８項に記載の２方向通信装置。

３３．（追加）前記再プログラム可能制御手段は少なくとも１つの電子的に消去可能なプログラム可能アレイ論理（ＥＥＰＡＬ）装置を具備する請求の範囲第８項に記載の２方向通信装置。

３４．（追加）少なくとも１つの前記ＥＥＰＡＬ装置は前記デジタル通信経路を介して外部プログラム装置によりプログラムされる請求の範囲第３３項に記載の２方向通信装置。

国際調査報告

International Application No PCT/US89/00002

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(4) H04K 1/00 U.S.Cl. 380/9, 28, 29, 49, 50

II. FIELDS SEARCHED

Minimum Documentation Searched

Classification System	Classification Symbols
U.S.	380/9,28,29,49,50

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched

III. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
Y	US, A, 4,004,089 (RICHARD et al) 18 JANUARY 1977 See Figure 1.	1-19
Y	US, A, 4,274,085 (MARICO, JR) 16 JUNE 1981 See Cols. 8 and 9.	1-19
A	US, A, 4,306,289 (LUHLEY), 15 DECEMBER 1981 See entire Document.	1-19
Y	US, A, 4,484,025 (OSTERMANN et al) 20 NOVEMBER 1984 See Figure 2.	1-19
Y	US, A, 4,598,170 (PIOSENKA et al) 1 JULY 1986 See Figure 7.	1-19
Y	US, A, 4,747,139 (TAAFFE) 24 MAY 1988 See Col. 3, lines 50-60.	1-19

IV. CERTIFICATION

Date of the Actual Completion of the International Search: 08 MARCH 1989

Date of Mailing of this International Search Report: 04 MAY 1989

International Searching Authority: ISA/US

Signature of Authorized Officer: Salvatore Cangialosi

第1頁の続き

⑫発　明　者	マツクラフリー・マイケル　ジエイ	アメリカ合衆国イリノイ州　60013、キヤリー、バース・ロード　114
⑫発　明　者	プール・ラリー　シー	アメリカ合衆国イリノイ州　60118、スリーピー・ホロウ、プラム・コート　6
⑫発　明　者	ブラウン・ダニエル　ビー	アメリカ合衆国イリノイ州　60126、エルムハースト、チヤサム・アベニユー　788
⑫発　明　者	ジオルコ・エリツク　エフ	アメリカ合衆国イリノイ州　60193、シヤンバーグ、サウス・フィーザント・ウオーク・ドライブ　810
⑫発　明　者	ブライト・マイケル　ダブリユ	アメリカ合衆国イリノイ州　60004、アーリントン・ハイツ、ノース・ミツチエル・アベニユー　1339

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)